

PROFISSIONAIS CIBERNÉTICOS DAS FORÇAS ARMADAS E DA INDÚSTRIA PRIVADA

Parceria em Defesa da Nação

Transcrição e Revisão:

Cap Jeffrey A. Martinez, *USAF*

Cap Matthew R. Kayser, *USAF*

Abaixo apresentamos um Diálogo entre a MajGen Suzanne Vautrinot, Comandante da Vigésima-Quarta Força Aérea e Charles Beard, Oficial Chefe de Informática, da *Science Applications International Corporation*

As discussões estratégicas referentes à cibernética não mais se restringem a diálogo acadêmico. A tecnologia associada não continua limitada aos laboratórios de desenvolvimento da indústria privada ou governamental. A “defesa” da arena cibernética é imperativo nacional. Os problemas complexos cada vez mais forçam os líderes empresariais e governamentais a expandir a colaboração para alcançar soluções viáveis. As empresas ao redor do globo utilizam o domínio cibernético para oferecer produtos e serviços com maior rapidez e a menor custo, equilibrando, ao mesmo tempo, a necessidade de proteger os dados pessoais dos clientes. É uma questão de confiança. Da mesma forma, os comandantes militares cada vez mais empregam a capacidade cibernética integrada para gerar efeitos cinéticos, ou não, em campos de batalha, bem como para comando e controle (C2). É indispensável ao sucesso da missão salvaguardar dados críticos, permitindo, ao mesmo tempo, maior acesso sem intercepções ou manipulações.

Dois líderes em cibernética, a MajGen Suzanne Vautrinot, Comandante da Vigésima-Quarta Força Aérea e Charles Beard, Oficial Chefe de Informática e Vice-Presidente da *Science Applications International Corporation - SAIC* tomaram parte em uma reunião no dia 7 de novembro de 2012. Durante a troca de ideias, Beard relatou a jornada empreendida pela empresa para reduzir a área vulnerável a ataques cibernéticos e o desenvolvimento de ambiente empresarial que resultaria

em solução tecnológica singular para a Informática. A MajGen Vautrinot, não só articulou similaridades existentes na Força Aérea para defender o ciberespaço nacional, mas também destacou como ambos, a Força Aérea e a Indústria Privada, podem empregar a experiência adquirida em empreendimentos bem sucedidos, como a migração da SAIC, à medida que continuam a encaminhar-se rumo à postura de cibersegurança mais homogênea.

Com o consentimento de ambos, compartilhamos o diálogo empreendido por esses dois colegas e parceiros que possuem mútuo reconhecimento e respeito nesse domínio dinâmico. Além do mais, inclui as contribuições de cada uma das Alas ciberespaciais da Vigésima-Quarta Força Aérea, elucidando pontos principais e colocando em destaque os empreendimentos atuais, a fim de operacionalizar e normalizar o domínio ciberespacial.

Vautrinot – Não surpreende o fato de que suas tentativas são semelhantes as nossas. Existe verdadeira similaridade de experiência na área. A sua empresa tomou elementos significativamente diversos e mudou a dinâmica completamente—organizacional e tecnologicamente. Estou interessada em saber que mudanças organizacionais predominaram. Gostaria de aproveitar [a oportunidade] para utilizá-las ao levar avante a responsabilidade compartilhada para com este ambiente global em fase de mudança.

Beard – Responsabilidade compartilhada é o termo correto. Quando observamos o domínio, reconhecemos que o estilo de gerenciamento deve mudar. Aumentamos o número de dependências a 10.000 escritórios independentes. Embora resultasse em vantagem para o desenvolvimento de mercado e reação positiva do consumidor, acabou acarretando desvantagens administrativas em grande escala (Informática). A agilidade estratégica é necessária para engajar mercados globais múltiplos em ambiente computacional cada vez mais hostil. O primeiro passo foi definir e estabilizar o ambiente. Assim, foi necessário mudar a maneira de pensar acerca da Informática.

Vautrinot – Da mesma forma, também podemos considerar os comandos principais e organizações práticas nas forças armadas—todos muito talentosos, mas também muito discretos (. . .) O termo “cilindros de excelência” vem à mente. Do ponto de vista de operações militares, isso tem sentido, mas causa dificuldades, quando nos dirigimos à ameaças e riscos cibernéticos. Uma vez que a tecnologia pertinente e os

meios de comunicação cresceram de forma descentralizada, existe aparente inércia em reter aquela abordagem descentralizada. Ainda assim, os senhores demonstraram a necessidade de criar uma solução empresarial para melhor operar o que denominamos de empresa cibernética.

Beard – Para nós, o primeiro passo foi fazer aquela conexão, a fim de assegurar que possuíamos verdadeiro ponto de vista empresarial do ambiente, começando a operá-lo como um recurso empresarial—sem preocupar-nos com sua origem. A próxima ação foi começar a trabalhar com o governo, debatendo a necessidade de compartilhar dados referentes à ameaça, a fim de aperfeiçoarmos a postura cibernética. A SAIC opera ambientes de Informática em nome do governo. Possuímos dados de clientes em nossas redes e assumimos a responsabilidade pela sua custódia com toda a seriedade possível. Ao mesmo tempo, é uma empresa de capital aberto, com operações globais. Não podemos simplesmente adotar um ponto de vista centralizado nos Estados Unidos para solucionar o problema. Da mesma forma, seria impossível para a Força Aérea assumir tal posição. Fomos obrigados a mudar a referência intelectual administrativa para muitos, o que para uma empresa multinacional significou confrontar, de verdade, a questão cibernética.

Vautrinot – Em esferas aéreas e espaciais, contamos com a vantagem de desenvolver sistemas singulares muitas vezes especializados e superiores: aeronaves de quinta geração em transição à sexta, bem como satélites de ponta (. . .) inerentemente únicos. O enfoque sempre foi em sistemas militares. Mesmo assim, o ciberespaço é um ambiente global interconectado. Compartilhamos o mesmo ambiente artificial. A indústria “de ponta” encontra-se no mesmo nível. As forças armadas não se podem dar ao luxo—técnica ou financeiramente—de reagir independentemente. Necessitamos de responsabilidade compartilhada—indústria privada, governo, instituições de ensino, parceiros internacionais— alterando o ambiente para vantagem coletiva, fazendo com que haja responsabilidade mútua para alcançar o sucesso. Em terminologia militar, podemos mudar o domínio para oferecer liberdade de movimento aos aliados e negar a mesma aos adversários. Todos nós operamos no mesmo espaço, embora seja necessário calcular o risco e a reação à missão de modo um tanto diferente.

[Nota da Redação:] A fim de executar os processos de planejamento teóricos, o Pentágono está dividido em estruturas organizacionais hierárquicas que representam grupos restritos de perícia (diretrizes, inteligência, análise de programa, aquisições e orçamento). Essas equipes estão subdivididas em áreas ainda mais especializadas. Há pouco tempo o pessoal brincalhão começou a denominar suas organizações de “cilindros de excelência” e o termo pegou, porque na verdade é exatamente isso. Seu propósito é criar e fomentar grande perícia em grupos bastante restritos de proficiência. Esses peritos identificam questões e formulam opções e recomendações, passando-as à cadeia de comando de alta patente. De acordo, o planejamento e a tomada de decisões movem-se, em essência, de baixo para cima, transitando, teoricamente, por um tipo de tubo vertical. Antigamente eram denominados “canais competentes”. No entanto, “canal” deixa a impressão de trânsito horizontal.

Beard – Tudo tem a ver com gerenciamento de risco e reação sistemática. Voltando atrás aos meus dias no Comando Aéreo Estratégico [*Strategic Air Command – SAC*] quando operávamos no domínio nuclear, a missão de dissuasão era bem clara. Também compreendíamos muito bem a missão de ataque. A ordem do dia era o prepativo para ambas. Ao contrário de outros domínios nas forças armadas—terrestre, aéreo, marítimo e espacial—a projeção de força e a supremacia em domínio cibernético são bastante difíceis. Estamos operando com estruturas compartilhadas globalmente, onde o adversário possui posição de igualdade e até mesmo mais avançada.

Vautrinot – Observo dinâmica global similar em nosso apoio à missões de VANTs. A fim de garantir a missão, fomos obrigados a levar a cabo extensa pesquisa avançada para compreender as várias conexões da sequência de voo dos Estados Unidos ao estrangeiro. O sistema foi projetado para mais ou menos 180 pontos de contato, muitos não controlados pelas forças armadas, através de várias redes distintas, inclusive sistemas estrangeiros. O estabelecimento de relações com organizações comerciais e aliadas foi crítico. A segurança e a garantia

são extremamente interdependentes, o que o senhor também nota na indústria privada.

Beard – Na esfera comercial a interdependência iguala a continuidade de operações e o gerenciamento de riscos. Existe uma diferença em como percebemos a ameaça, mas a garantia da missão para dada empresa comercial é impulsionada, em grande parte, pelos mercados e posição geográfica em que operam, bem como o tipo de operações levado a efeito. O fato de que essas operações são realizadas em infraestrutura globalmente compartilhada é contexto importante que os executivos empresariais devem compreender, à medida que consideram os riscos.

Vautrinot – Os comandantes que apoiamos indicaram imperativo similar para acesso ininterrupto a dados confiáveis e passíveis de verificação. A garantia da esfera cibernética é tão fundamental à missão que não podemos nos dar ao luxo de perder a capacidade de comunicação—é essencial ao comando e controle militares.

Beard – Correto. Pode ser que dada empresa possua a melhor capacidade do mundo, mas mesmo assim, não consegue operar na esfera digital. Se não conseguir sustentar acesso ininterrupto à energia e à infraestrutura de comunicação é muito difícil contar com a sobrevivência da missão. Assim percebemos a grande similaridade entre comando e controle de missões militares e privadas, porque estamos tentando levar a efeito operações comerciais ao redor do globo. Se não consigo providenciar acesso à comunicações claras e energia ininterrupta, a continuidade comercial é prejudicada de forma dramática.

Vautrinot – Na esfera empresarial, deve-se ir além de conscientização. É necessário que as pessoas tomem parte ativa, compreendam a co-dependência e notem seu benefício para com o indivíduo. O debate em menor escala faz com que o efeito seja tangível e com que a mudança seja aceita. Uma empresa bem sucedida pode fazer uso disso para tomar novos rumos. Será que a percepção foi algo feito sob medida para cada indivíduo e depois ampliada, ou será que a liderança foi obrigada a impulsionar a conscientização da empresa, a fim de alterar o legado organizacional?

Beard – Na SAIC, tivemos a vantagem de contar com pessoas que possuem experiência em governo e indústria e que compreendem o fato de que a ameaça existe. Assim, começamos a traduzir aquele risco ao contexto comercial. Creio que o que descobrirá é que diversas indústrias comerciais já avançaram bem nesse sentido, já passaram por aquela experiência. É claro que a indústria especializada em serviços financeiros

está ciente do fato. Possui comitês dedicados ao estudo de risco em seus conselhos administrativos e é um dos muitos obstáculos que deve levar em consideração. Existem outras indústrias, como a de energia, onde a tomada de consciência está aumentando cada vez mais. Presenciam a trajetória da ameaça, mudando de simples compilação de inteligência à destruição operacional, como indicado pelo caso *da Saudi Aramco*.¹ Na esfera médica, pode ser que dada empresa passe uma década, gastando 10 bilhões de dólares para desenvolver produto ou medicamento, somente para ver sua cópia carbono ser lançada em país estrangeiro um ano antes da obtenção de autorização da *Food and Drug Administration – FDA*. Toda sua propriedade intelectual desaparece. Assim, a renda antecipada pela empresa para aquele produto para os próximos 10 anos é significativamente mais baixa. Os imperativos econômicos transformam-se em perigo real e imediato à economia nacional onde essas empresas operam, mas muitas ainda não compreendem as ameaças cibernéticas e seus possíveis impactos, tanto físicos como econômicos.

Vautrinot – Existe reconhecimento similar acerca da dependência cibernética. Contudo, não estou segura de que existe a percepção referente ao grau de dependência e nossa habilidade de levarmos a efeito todas as missões que são—voar, lutar e vencer no ar, espaço e ciberespaço. A demanda, à medida que avançamos, é criar um vínculo entre todos os elementos da missão (. . .) a tapeçaria operacional verso os fios da missão. À medida que expandimos o enfoque, devemos estar cientes disso para que haja o equilíbrio entre as tentativas operacionais e a habilidade de manter e defender as redes. A Vigésima-Quarta Força Aérea [*Twenty-Fourth Air Force*], a 689ª Ala de Comunicações de Combate [*689th Combat Communications Wing*] especializa-se em manter esse equilíbrio, ampliando a capacidade cibernética ao perímetro tático, em apoio ao combatente, ao mesmo tempo em que continua a oferecer comunicações defensíveis e confiáveis àquele perímetro.²

Beard – O fato é que certos usuários simplesmente não compreendem que o correio eletrônico é transmitido a servidores além das redes de nossa empresa e das fronteiras nacionais—talvez a países cujas leis de interceptação sejam diferentes das nossas. Erigimos todo tipo de empresas que dependem de cibernética, mas não compreendemos, na realidade, os problemas de segurança associados àquele domínio. Quando começamos a compreender o tipo de impacto real, vemos que é algo que intimida. Isso porque a liderança é essencial para podermos navegar pelo labirinto e extensão sem fim da confiabilidade de rede.

Vautrinot – No ambiente orçamentário atual, existe um fator que complica a situação: o comprometimento esperado dos recursos, na verdade, põe um fim ao diálogo e ao espaço para a tomada de decisões, antes que possamos explorar as opções disponíveis. A complexidade da transformação no ambiente empresarial vem a ser sua própria inércia. Se a cibernética está desordenada, ficamos então entalados entre a “entropia” natural do domínio e a inércia da decisão. A sua empresa foi obrigada a enfrentar esse tipo de situação?

Beard – Há pouco tempo ouvi um advogado sugerir que não era necessário para os membros do Conselho Administrativo ficarem bem informados acerca dos riscos em segurança cibernética porque as leis garantem a proteção daquilo que não sabem. Acho que é um ponto de vista bastante bitolado. Creio que no contexto do comércio privado—por exemplo, um banco, ou empresa de utilidade pública, indústria farmacêutica ou que possua contratos em defesa—a base dessas empresas é sua reputação e confiabilidade. Os conselhos administrativos das empresas pertinentes que exibem práticas sólidas em gerenciamento de riscos, sabem muito bem se estão em posição segura para julgar esses riscos. Para nós, o risco cibernético talvez seja o perigo principal que encaramos. No entanto, para um empreiteiro na indústria privada de defesa, pode ser que o maior risco seja o grupo de pessoas que se encontra em perigo de vida. Para uma instituição financeira seria crise de liquidez. A farmacêutica preocupa-se com a aprovação da *FDA*, a fim de fazer face às estimativas de vendas e ir ao encalço das cópias falsificadas de seus produtos que estão sendo piratadas ao redor do mundo. A questão é a boa articulação desse tipo de risco. A noção de que só basta erigir uma fortaleza ao redor do negócio, com defesas cibernéticas estáticas é simplesmente a versão digital da Linha Maginot.

Vautrinot – Concordo, as defesas estáticas não funcionaram durante a Segunda Guerra Mundial e não funcionarão em ambiente cibernético. Este é o motivo pelo qual na Força Aérea, o enfoque é em postura de defesa proativa. Não podemos esperar que um adversário penetre as redes para avaliarmos as vulnerabilidades. Estabelecemos equipes especializadas que varrem as redes em busca de vulnerabilidades, preferivelmente antes que sejam exploradas. O enfoque é identificar e defender aquelas interfaces essenciais ao sucesso da missão—O Gen Keith Alexander, Chefe do Comando Cibernético dos Estados Unidos [*US Cyber Command*], denomina essa capacidade de “reconhecimento /contra reconhecimento” [*recon/counter-recon*]. Uma faceta principal dessa tentativa é identificar e manter o enfoque em uma

“lista de recursos defendidos” [*“defended asset list”*] priorizados pelo Chefe, i.e., aquelas áreas essenciais que são obrigadas a operar durante ambiente contestado ou ataque. Isso bate diretamente com algo que já havíamos discutido: vincular as tentativas feitas contra a missão operacional. Poderíamos acessar um ambiente de rede e fornecer ao comandante que depende daquele sistema, dados precisos para tomada de decisão. Especificamente, será que ele pode basear-se no sistema de redes para cumprir a missão com êxito?

Essa postura proativa é apoiada pela partilha de vetores de dados e de ameaças entre a indústria e o governo. Um exemplo excelente é o Programa de Defesa Voluntária da Segurança Cibernética da Base Industrial do Departamento de Defesa / Garantia de Dados [*Department of Defense’s Voluntary Defense Industrial Base Cyber Security / Information Assurance Program*], um acordo pelo qual as empresas, que incluem uma série das maiores do país, colaboram com o Departamento de Defesa na Força Aérea, via a Equipe de Reação à Emergências em Informática da Força Aérea [*Air Force Computer Emergency Response Team*] sob a 67^a Ala de Guerra em Rede [*67th Network Warfare Wing*] e o Departamento de Segurança do Território Nacional [*Department of Homeland Security*], a fim de compartilhar dados sensíveis de ameaça para aperfeiçoar a defesa ciberespacial coletiva.³

Beard – O que começamos a notar agora, no setor empresarial, é a frustração de mantermos uma defesa estática. O tráfico subjacente de ataques cibernéticos atualmente favorece o adversário, da mesma forma que os dispositivos explosivos improvisados favorecem os insurgentes. Em contrapartida àquele modelo, entramos em parceria com a indústria e o governo, para o desenvolvimento de plataformas confiáveis que permitam defesas dinâmicas através de nossos produtos marca *Cloudshield*. Alternativamente, certas pessoas no mercado creem que está na hora de começar a revidar. Essa nova perspectiva é passar de defesa de rede à ataque. A minha preocupação é grande acerca de empresas particulares que assumem missões de ataque à redes de informática, com consequências extemporâneas, tanto para as agências encarregadas de fazer cumprir com a lei, como para outras agências governamentais.

Vautrinot – Geralmente, de acordo com as leis internacionais, o conceito de ataque fazia parte da responsabilidade das diferentes nações. No entanto, os limites geográficos não mais demarcam os protagonistas na ofensiva. Por exemplo, observamos empresas que alegam vender proteção em reação à interferência cibernética com o envio de comandos

de reinicialização ou redirecionamento do tráfego virulento. A natureza cibernética é que as empresas podem muito bem possuir a capacidade de ir além. Com isso, entrarão em conflito com as leis e estatutos éticos onde operam ou produzem efeitos. Infelizmente, as atuais diretrizes domésticas e internacionais não mantêm passo com os avanços em capacidade cibernética. Assim, existem cláusulas de derrogação e meios de escape, sem falar de lacunas administrativas gritantes que podem ser utilizadas por empresas audazes.

Na Força Aérea, a restrição não só existe em códigos de lei domésticos, mas também em diretrizes governamentais. Em geral, o Departamento de Proteção do Território Nacional é responsável pela defesa de recursos cibernéticos fora das redes do Departamento de Defesa. No entanto, não importa a organização envolvida. Os problemas são muito difíceis, quando tentamos atribuir uma invasão de rede a determinado agressor para decidir que agência será designada a tomar as ações necessárias. Isso, uma vez mais, destaca a necessidade de estrutura preestabelecida de partilha de dados entre o governo e a indústria privada que facilite a rápida ação contra eventos cibernéticos.

Os líderes de alta patente da Força Aérea certamente estão cientes das vulnerabilidades dos sistemas de rede nacionais, mas agora também existe intenso reconhecimento das oportunidades de capacitar a defesa e facilitar o sucesso da missão. Um grande exemplo foi o trabalho junto ao Comando de Transporte dos Estados Unidos [*US Transportation Command*] e o Comando de Mobilidade Aérea [*Air Mobility Command*]. Suas conexões não se limitam ao domínio *.mil*, mas também ao *.com*, bem como a habilidade de trabalhar com os parceiros industriais, a fim de assegurar movimento mundial. O resultado é que estão profundamente cientes da situação e isso impulsiona sua proatividade em termos de resolução. Ainda assim, em outros comandos existe resistência e crença de que suas redes são “privadas” ou separadas da *Internet* global e de seus inerentes adversários. Com respeito aos gabinetes independentes, o senhor percebeu o mesmo tipo de discrepância?

Beard – Sim, de fato. Contávamos com empregados, associados e até mesmo clientes que operavam de acordo com o que acreditavam ser “redes fechadas”. Assim, pensavam que não havia problema. Simplesmente não percebiam a necessidade de adicionar outras camadas de proteção ou fazer cumprir com as diretrizes referentes a suas atividades. O que denominavam de burocracia é o que denominamos de garantia de missão dentro do contexto de engenharia de sistemas.

Vautrinot – Sem dúvida, uma necessidade de união de esforço e com ele uma cadeia de responsabilidade bem definida—comando e controle. Certamente, os senhores estavam colocando em execução uma solução empresarial de acordo com motivos justificados e área de escritórios independentes notou essa importância. No entanto, existe resistência à perda daquilo que certas pessoas creem ser sua auto-realização—sua habilidade de controle. O que foi que lhe permitiu superar aquela resistência natural em campo e impulsionar a execução?

Beard – Diria três coisas: a primeira foi o compromisso para com a liderança: “estamos dispostos a fazer isso”; segundo, começamos a educar a liderança, gerência e grupos selecionados de empregados. Para nós foi algo de suma importância—o aumento de conscientização; finalmente, fomos obrigados a ver o contexto de segurança cibernética de outra forma. Foi necessário compreender aquilo que é imprescindível proteger e onde devemos estabelecer a confiança. Os resultados daquele exercício mudaram completa e materialmente a estratégia de defesa.

Vautrinot – Que graus de liderança foram necessários? Para nós seriam os comandos e práticas principais. Após o que podemos declarar, “Muito bem, estamos todos de acordo. Reconhecemos a ameaça e vamos todos caminhar rumo à mesma direção”. Assim, é nossa responsabilidade ajudá-los a compreender a justificativa para colocar em execução as medidas ou tomar a ação que pode ser localmente restritiva.

Beard – Correto, nem todos estiveram de acordo. Levou um grupo combinado composto de um oficial executivo chefe/oficial de operações chefe/oficial financeiro chefe e daí então partimos para o quebra-caco.⁴ Embora as pessoas compreendessem a decisão da liderança e a necessidade de fazer cumprir com as diretrizes, bem como monitoria, ainda assim desejavam autonomia. Desenvolvemos, então, dispositivos para oferecer autonomia, ao mesmo tempo preservando a postura de segurança. Isso foi feito no contexto de produtividade, providenciando ao pessoal aquilo que desejavam. O que foi impossível compreender 20 anos atrás, quando as operações no domínio digital começaram a evoluir, foi esta questão de risco cibernético. Surge agora como um espectro e não pode mais ser ignorada. Portanto, estamos em conflito. Meu desejo é proteger o usuário final, como cliente. No entanto existe outra responsabilidade: Pode ser que o cliente compreenda ou não, mas tento explicar. É impossível abranger todos os usuários, porque não conto com os meios necessários. Como poderia desincumbir meus outros deveres?

Vautrinot – Os senhores estão protegendo a viabilidade da entidade empresarial a longo prazo, da mesma forma que estamos

protegendo a viabilidade da missão e nosso apoio à nação, a longo prazo. Deve existir certa liberdade de ação em toda a empresa que permita tal proteção.

Creio que na indústria privada também existe o requisito de documentar, via relatórios, não a segurança cibernética em si, mas sua viabilidade como entidade empresarial na esfera da segurança cibernética. Se eu tivesse que fazer o mesmo, calculo que seríamos reprovados. No entanto, estamos nos movimentando rumo a conceito, onde existe gerenciamento, tanto na esfera de recursos, como na empresarial, mas somente nas redes *.mil* e *.seu*. Cada uma das redes de sistema de missão é definida separadamente e possui recursos e administração independentes. Em seu modelo, [por exemplo] haveria um “general” designado para controlar o gerenciamento de recursos para todas as interfaces das redes da Força Aérea, do início ao fim—precisamente o que os senhores foram obrigados a fazer na empresa privada. Certamente algo necessário, mas aprendi que a viabilidade operacional neste ambiente contestado requer mudança fundamental em recursos que seriam administrados centralmente—isso requer a utilização de sensores para capacitar a conscientização e reação proativa à ameaças dentro da rede. O primeiro passo – o gerenciamento de recursos – por si só é insuficiente, mas com os sensores – a fim de obtermos aquela percepção da situação para fazer com que o sistema reaja automaticamente—é o próximo passo. Como abordaram os senhores as mudanças em engenharia?

Beard – Isso fez parte da segunda jornada do processo—a instrumentalização e a análise de todas as vulnerabilidades da empresa e o escrutínio minucioso comparado àquela linha de base. Isso permitiu o preparo para a monitoria contínua. O motivo de sua importância levamos ao terceiro passo: Pode ser necessário *metamorfosear* [*morph*] minha rede, tendo como base a missão empresarial, dados de inteligência relacionados à ameaça acionável e o intuito de selecionar adversários ativos.

Vautrinot – Isso é onde as operações cibernéticas podem facilitar as operações da missão ou providenciar alternativas à mesma. Não necessitamos comandar e controlar a missão, mas devemos possuir visibilidade completa daquilo que está ocorrendo no ciberespaço e a capacidade de fazer os ajustes em tempo real para frustrar o posicionamento do inimigo. Isso dificulta muito mais os problemas encarados pelo inimigo e ao mesmo tempo preserva a eficácia da missão.

Beard – Exatamente. Porque se os adversários conhecem e compreendem sua rede melhor do que a Força Aérea, aí sim vão enfrentar problemas, e se a infraestrutura dos seus computadores for tão rígida que previne a alocação dinâmica, eles tomarão vantagem da situação. Daí então, uma vez mais as vantagens econômicas e operacionais estarão do lado do adversário. Foi por isso que mudamos para o modelo *hybrid cloud*—porque oferecia a oportunidade de movimentar as cargas de trabalho na esfera de dados e aplicação. Podemos agora tomar uma carga que normalmente operava via servidores específicos em um centro de dados específico e de forma dinâmica e designá-la a equipamento virtual que opera em centros de dados virtuais e em regiões geográficas bem distintas. A informação pode permanecer dentro do centro de dados, mas posso movimentá-la a diferentes lugares.

Vautrinot – De acordo com esse conceito, por exemplo, o tratamento de saúde de empregados não conta com dados médicos e o departamento financeiro não possui dados financeiros. A movimentação e o fornecimento de acesso a dados desejáveis dentro da empresa é o essencial. Cada departamento possui acesso aos dados, porém sem controlá-los como elemento segregado. O objetivo não deveria ser controlar, mas sim fazer com que dados confiáveis estejam à disposição a qualquer hora, em qualquer lugar. O problema é criar um ambiente continuamente ágil.

Parece que o termo “economia” em eficácia *IT* seja um tanto inapropriado. Quando entramos em contato com a *AT&T*, *Microsoft* e parceiros industriais, como o senhor, o investimento inicial para agilizar essa mudança não é somente um investimento em cultura e liderança empresariais, mas também em capital. Não só para economizar dinheiro durante toda a operação *IT* a longo prazo, mas um investimento financeiro *IT* em segurança cibernética. Como foi que sua empresa operou durante a dinâmica de investimento para determinar se a segurança cibernética seria um imperativo financeiro para a empresa? Qual foi a extensão daquela avaliação e diálogo?

Beard – Durante o investimento inicial o enfoque definitivamente não foi economizar, mas sim investir em agilidade estratégica e saber o que significaria para um empreendimento como o nosso – i.e., uma empresa global. Sabíamos que necessitávamos de agilidade em esfera empresarial. Assim, o objetivo foi a flexibilidade. É útil manter em mente não só a utilização da tecnologia, mas também como virtualizar as empresas, recombinação-as. Na verdade, a *SAIC* está passando por esse

tipo de processo agora mesmo. A *IT* deve ser vista como benefício e não como obstáculo a sobrepujar.

Vautrinot – A cibernética no contexto que descrevemos é uma missão e a viabilidade (de operação) sem ela, não existe. Apesar da situação econômica nacional que agora enfrentamos, devemos fazer com que o diálogo passe de redução de custo a imperativo de defesa e seja, assim, digno de investimento do ponto de vista da estratégia nacional.

Beard – Do ponto de vista orçamentário separamos a cibernética do geral, tratando-a como investimento estratégico. Se percebermos a *IT* como item de despesa a oportunidade desaparece. Através dos anos assessoriei uma série de empresas que buscavam reduzir o custo da *IT*, a fim de alcançar a meta orçamentária. No entanto, o segredo que ninguém revela é que acabavam assumindo a dívida técnica que não faz parte do balancete (déficit não financiado) e que também não é registrado como risco empresarial.

Vautrinot – Segundo a lógica, minha “dívida técnica” é a falta de automatização e presença de sensores, o que faço manualmente – de fato, uma mão-de-obra enorme não sustentável ou apropriada a ambiente cibernético dinâmico. Isso exige outras operações, a fim de reagir a problemas e inibe a aquisição de soluções, recursos e sensores automáticos.

Nossas tentativas de passar de rede dispersa, gerenciada pela dependência à rede única, homogênea e administrada centralmente permitirão o seguimento com os necessários sensores e automatização para liberar os recursos e operações robustas em rede, imprescindíveis à indústrias globalizadas, como a sua e à operações militares. Até então, tudo isso garante enorme custo final.

Beard – Todos sabem que uma postura reativa é mais cara. Jamais faríamos isso com um empreendimento de desenvolvimento de sistema de armas—tentamos projetar engenharia sólida logo no investimento inicial. É muito mais econômico, a longo prazo.

Vautrinot – A suposição é de que, no mínimo, podemos solucionar aquilo que podemos ver. Mas que tal aquilo que completamente desconhecemos?

Beard – Isso sim é inaceitável. Para propósitos da Lei [*Sarbanes-Oxley Act*], por exemplo, requer-se a instalação de controles pertinentes.⁵ Aquilo que desconhecemos força-nos a raciocinar antes de agir, antes que a tensão se torne violenta [*“left of bang”*]⁶. Mas isso então nos leva a perceber que não podemos proteger tudo. Assim, que tal um diálogo de

negócios ou assuntos militares acerca de recursos—como recursos de dados—que desejamos proteger.

Vautrinot – É o que denomino de lista de recursos defendidos, mas de forma abstrata e não empresarial. Trabalhamos individualmente com o Centro de Controle de Transporte Aéreo de Tanques [*Tanker Airlift Control Center – Planeja, agenda e dirige frota de mais de 1.300 aeronaves em apoio a combate para transporte aéreo estratégico em combate e evacuação aeromédica*], bem como com um dos muitos centros de operações, a fim de demonstrar tal dinâmica. Mas não podemos empregá-la no setor empresarial porque não podemos “ver” ou controlar os recursos cibernéticos da empresa.

Beard – Às vezes, no escritório, recebo uma chamada: “Estou com este problema urgente de segurança. Ajude-me, por favor.” As primeiras perguntas que faço são: “Quando foi que percebeu que devia proteger o recurso?” e “Quando soube que havia um problema?” Se não estava na lista de recursos defendidos, nada fiz proativamente em termos de proteção, e se foi exfiltrado ou manipulado, especificamente, não tentei assegurar sua saída ou preservar sua linha de base. Assim, se a lista de recursos defendidos estiver incompleta é bem difícil desenvolver e colocar em execução uma diretriz cibernética para proteger e defender aqueles recursos. Aqui, o jogo é de equipe. É a responsabilidade compartilhada para garantir missões incrivelmente dinâmicas. Simplesmente, se acabamos de adquirir um aplicativo de segurança, no momento em que é colocado em operação, já está obsoleto. Assim, existe uma ameaça assimétrica, quando se tenta reagir segundo processo tradicional. É contraproducente. É por isso que estamos tentando mudar o jogo.

Vautrinot – Exatamente. É por isso que estamos construindo uma plataforma constantemente adaptável. Para fazer uma comparação com as operações espaciais, defino a interface da carga útil como a plataforma. Isso quer dizer que sou a proprietária da plataforma e da empresa e posso adaptá-la em tempo real. Por exemplo, sob o Cel Paul Welch, o Comandante da 688^a Ala de Operações de Informática [*688th Information Operations Wing*], projetamos a Plataforma de Operações de Informática [*Information Operations Platform*], a fim de oferecer uma estrutura aberta e bem acreditada para o rápido lançamento de outros aplicativos de terceiros.⁷ Essa habilidade de permutar os dispositivos permite seu rápido destacamento e posicionamento em campo, oferecendo operações dinâmicas e reativas para a Força Aérea e para as operações ciberespaciais do Departamento de Defesa. Oferece flexibilidade—como caça leve, que pode ser configurado para *ar-terra* em

dada missão e para missão *ar-ar* em outra. A diferença é que se reconfigura o caça para atuar durante horas/dias, enquanto que em cibernética a reação deve ocorrer em questão de segundos.

Beard – Digamos que meu sistema de detecção de invasores tenha sido penetrado e necessito de algo novo. A base de programas (*software*) faz parte de uma plataforma e não é negociável, assim a plataforma (*hardware*) do equipamento em si, não muda. Posso destacá-la agora mesmo. É esta máquina sigilosa com controles fora de banda que só nós podemos ver, mas que nela consigo colocar diferentes cargas úteis.⁸ Os escritórios independentes podem fazer o que devem, mas a empresa ainda assim domina a rede dos mesmos. É o truque—comando e controle em esfera empresarial com execução descentralizada, um ambiente dinâmico que oferece agilidade à empresa e cria “confiança” na plataforma que é altamente configurável e que permite vigilância antes do início das hostilidades.

Vautrinot – A intenção é de que à medida que continuamos a refinar nossa habilidade neste domínio vamos passar de postura reativa à proativa e apresentar alvos ágeis, providos de sensores, aos adversários. Todos nós, governo ou indústria privada, fazemos parte do mesmo tipo de negócio: Confiabilidade. E devemos utilizar o capital intelectual disponível e a tecnologia de ponta para proteger a informação e sistemas, a fim de evitar que sejam vinculados à amplas cadeias maliciosas [o custo global para remediar o problema em 2011 foi de \$388 bilhões de dólares].⁹ A jornada cibernética da nação é responsabilidade compartilhada e é pessoal—somente através do desenvolvimento de parcerias podemos continuar a defender esta nação no ciberespaço.

É difícil compreender o âmbito sem fim deste domínio. Durante os próximos 60 segundos: o correio eletrônico enviará 168.000.000 mensagens; o *Facebook* atualizará 695.000 dados; e o *Google* processará 690.000 buscas.¹⁰ À medida que as oportunidades oferecidas continuarem a aumentar geometricamente, assim também as vulnerabilidades.

Aqueles presentes saíram da sala não só com um melhor entendimento das dificuldades futuras, mas também com maior reconhecimento do trabalho colaborativo entre o governo e a indústria privada para salvaguardar os dados essenciais nos quais se baseiam as empresas, os comandantes das forças armadas e a nação.

Notas

1. No dia 15 de agosto de 2012, em uma das ações mais destrutivas de sabotagem em informática, um vírus apagou os dados de três-terços dos computadores da *Aramco*, uma empresa da Arábia Saudita, substituindo os dados com uma bandeira norte-americana em chamas. Devido ao ataque, a empresa foi forçada a substituir dezenas de milhares de discos rígidos.

2. A missão da *689th Combat Communications Wing* é treinar, destacar e suprir comunicações especializadas e expedicionárias, controle aéreo e sistemas de aterrissagem durante operações humanitárias, de assistência e de combate, a qualquer hora, em qualquer lugar. Para manterem-se atualizados com o ambiente estratégico em rápida mudança, os comunicadores em combate baseiam-se em grande parte na indústria para o suprimento de tecnologia a varejo, que torna possível a operação, defesa e expansão da capacidade cibernética nos locais mais áusteros e da maneira mais eficaz possível.

3. É um desafio constante assegurar a defesa de dados e sistemas militares – por meio de defesa e ataque de redes de informática. A *67th Network Warfare Wing* executa operações de rede para a Força Aérea, defesa, ataque e exploração, a fim de criar efeitos ciberespaciais integrados para a *Twenty-Fourth Air Force* e os comandantes combatentes. A Ala opera segundo os documentos de autorização atualizados do Departamento de Defesa para proteger os dados e sistemas da Força Aérea e do *DoD* e, a fim de assegurar liberdade de manobra no domínio cibernético. A *67th* inclui os operadores da rede responsáveis pela operação diária das redes da FA. Extensa colaboração entre o pessoal da Ala e outras organizações civis e governamentais assegura a partilha contínua de dados de ameaça cibernética através de entidades públicas e particulares.

4. Da mesma maneira que um “toro em loja de porcelana” estilhaça a mercadoria, neste caso, a introdução de processos de segurança cibernética rompeu os processos do comércio normal.

5. Existe um projeto de lei do Congresso, colocado em vigência em 2002, a Lei *Sarbanes-Oxley*, no Senado denominada de Reforma de Contabilidade de Empresas Públicas e Lei de Proteção ao Investidor, e na

Câmara dos Vereadores de Lei de Responsabilização e Auditoria Empresarial e Lei de Responsabilidade [*Corporate and Auditing Accountability e Responsibility Act*]. Esse foi colocado em vigência, devido a série de grandes escândalos empresariais e de contabilidade, inclusive aqueles da *Enron* e *WorldCom*.

6. O termo *left of bang* refere-se a período de tempo durante o qual cada incidente marcado é um “banguê.” Atividades à direita [após] do banguê [*right of bang*] são reações ao incidente. As *left of bang* são ações proativas em preparativo para tais eventualidades.

7. A *688th Information Operations Wing* providencia essas operações comprovadas de dados e capacidade de estrutura (engenharia) integradas através do ar, espaço e ciberespaço. Essa Ala desenvolveu processo de desenvolvimento de ferramenta rápido acompanhado de programa de aquisição acelerado que reflete abordagens imediatas a médio e longo prazos. A estrutura de inovação envolve o *Air Force Materiel Command (AFMC)* operando junto com o *Air Force Space Command*, a fim de estabelecer um centro para inovação cibernética para providenciar capacidade cibernética eficaz a preço razoável, tais como a Plataforma de Operações de Informática [*Information Operations Platform*], dentro do período de tempo apropriado para apoiar o combatente conjunto.

A *688th* expande as inovações alcançadas pelo tópico de interesse da pesquisa, patrocinadas pelo Coronel Welch, ao entrar em parceria local com a perícia em ciências e tecnologia do Laboratório de Pesquisa da Força Aérea [*Air Force Research Laboratory*] simultaneamente unindo-se aos pares em aquisição, tais como o Cel Chris Kinne, do *AFMC* em San Antonio, a fim de expandir a autoridade de aquisição local delegada pelo Gabinete do Secretário da Força Aérea, Encarregado de Aquisição, [*Office of the Secretary of the Air Force for Acquisition*]. Requer-se grupo estabelecido e diversificado em conhecimento para complementar a perícia do departamento em desenvolvimento cibernético. O TenCel Jim Smith lidera a presença do Centro de Provas Operacionais e Avaliações da Força Aérea [*Air Force Operational Test and Evaluation Center*] nesta nova organização, a fim de testar e verificar a eficácia das capacidades propostas em ambientes operacionais.

8. O controle fora de banda passa os dados de controle em conexão separada dos dados principais.

9. *Norton Cybercrime Report 2011*, Symantec Corporation, 7 September 2011, http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/.

10. “60 Seconds—Things That Happen On Internet Every Sixty Seconds,” GO-Gulf.com, 1 June 2011, <http://www.go-gulf.com/blog/60-seconds/>.